U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371***		*Attorney's Docket Number* MODL3003/JEK *U.S. Application Number (if known)* 10/030162
International Application Number PCT/EP00/07122	*International Filing Date* 25 July 2000	*Priority Date Claimed* 30 July 1999
Title of Invention METHOD, DATA CARRIER AND SYSTEM FOR AUTHENTICATION OF A USER AND A TERMINAL		
Applicant(s) for DO/EO/US Albert MODL et al.	Assignee	

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.

3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).

4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☒ A translation of the International Application into English *(35 USC 371(c)(2))*.

7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.

9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. (☐ Executed ☒ Unexecuted)

10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

Items 11 to 16 below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.

13. ☐ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☒ Other items or information: 1 sheet formal drawing

Application Number (if Known)	International Application Number	Attorney's Docket Number
10/030162	PCT/EP00/07122	MODL3003/JEK

	Calculations	PTO USE ONLY
17. The following fees are submitted: **Basic National Fee** *(37 CFR 1.492(a)(1)-(5))*: ☒ Search report has been prepared by the EPO or JPO . . . . . $890.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* . . . . . $710.00 ☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* . . . . . $740.00 ☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO . . . . . $1040.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT	$ 890.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.		

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	12	-20 =		× $18.00		
Independent Claims	2	-3 =		× $84.00		
Multiple Dependent Claims (if applicable)				+ $280.00	$ 280.00	
				TOTAL OF ABOVE CALCULATIONS	$ 1,170.00	
Reduction by ½ for filing by small entity, if applicable. Small Entity Status is asserted pursuant to 37 CFR 1.27 for this application.						
				SUBTOTAL	$ 1,170.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.						
				TOTAL NATIONAL FEE	$ 1,170.00	
Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property.						
TOTAL FEES ENCLOSED					$ 1,170.00	
				Amount to be:	Refunded:	
					Charged:	

a. ☒ A check in the amount of **$1,170.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

Customer 23364

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 30 January 2002

Respectfully submitted,

J. Ernest Kenney
Attorney for Applicant
Registration Number: 19,179

Method, data carrier and system for authenticating a user and a terminal

The present invention relates in general to authentication for the use of data carriers such as smart cards and the like, and in particular to an authentication method, a data carrier and an authentication system comprising a data carrier and a terminal.

To prove that a user is actually entitled or authorized to use a smart card or magnetic stripe card, an individual secret number, for example a so-called PIN (personal identification number) is customarily used. The PIN is stored on the card and, after the card has been introduced into a terminal, compared with the PIN entered in the terminal by the user. If comparison is positive the terminal can e.g. access protected areas of the smart card, for example memory areas.

The use of PINs is problematic because the card can be used by anyone with knowledge of the PIN. The card is thus not bound to the actual card holder but to the PIN holder. Voluntary or involuntary transmission of the PIN thus makes it possible to abuse the card. PINs are also unsafe insofar as they can be forgotten, on the one hand, and spied out, on the other hand.

Even when an authorized user has identified himself by entering his PIN, the system is only partially authorized - that is, the user with respect to the card and to the terminal. There is no authorization of the terminal with respect to the card or to the user. If the terminal is fake there is a danger of the PIN being spied out by the fake terminal. The PIN alone therefore does not constitute sufficient protection because there is no authentication of the terminal with respect to the card or to the user.

US 5,239,166 discloses a system for safe data exchange comprising a card and a terminal. In the known system the card and the terminal check each other. The user of the card is checked by means of biometric features, e.g. a fingerprint.

US 5,208,447 discloses a method for checking terminals with a smart card wherein a password stored in the smart card is transmitted to the terminal in both encrypted and unencrypted form. The encrypted password is decrypted in the terminal and compared with the password transmitted in unencrypted form. If the decrypted password matches the unencrypted password, the terminal is authorized.

The present invention is based on the problem of making the authentication process safer. In particular, the problem underlying the invention is to propose an authentication method, an authentication system comprising data carrier and terminal, and a data carrier for authenticating both the user and the terminal, thereby permitting the user's individual authorization and the authenticity of the terminal to be checked.

This problem is solved according to the invention by an authentication method, a data carrier and an authentication system according to the independent claims.

The subclaims state advantageous embodiments of the invention.

The inventive solution is based on the idea that the authentication process can be made safer if the authenticity of the terminal is first checked and the terminal is then presented with biometric data of the user. Biometric data, such as a fingerprint or the like, are clearly user-specific, unlike a PIN. The prior check of the terminal's authenticity guarantees that the sensitive, user-specific biometric data cannot be spied out. The terminal's authenticity is checked by a secret code permanently stored on the data carrier and known only to the user being read by the terminal and displayed to the user. Only if the secret code is displayed correctly does the user present the biometric feature to the terminal to identify himself as an authorized user to the terminal and the data carrier. The secret code can be stored on the data carrier on a memory location that can be accessed only by authorized terminals and/or be decrypted correctly only by an authorized terminal.

After the terminal has been authenticated, user-unique authentication with respect to the data carrier and to the terminal is obtained by presentation of the user-specific biometric feature and comparison of the data detected from the biometric feature with biometric data stored on the data carrier, in contrast to PIN comparison.

In addition to biometric authentication of the user, a PIN authentication of the user can be effected by entry of a PIN and comparison of the entered PIN with the PIN stored on the data carrier.

The invention will be set forth in the following by way of example with reference to the single figure.

The authentication process shown in the figure includes three steps, of which the second step can be omitted.

In the first step, terminal *T* reads a secret code (*CODE*) from a first memory area of data carrier *C*, for example a smart card, and presents said *CODE* to user *U*. *CODE* is stored on smart card *C* for example on a protected-access memory location and/or in encrypted form, so that *CODE* can only be read and displayed to user *U* by "real" terminal *T* which either has access authority or knows the decryption algorithm.

If user *U* recognizes *CODE* read by terminal *T* as his secret code, he will perform the further authentication steps. In the shown case, he will first enter his PIN in terminal *T*. The PIN is then transmitted, preferably in encrypted form, to smart card *C* where it is decrypted and compared with a PIN stored on smart card *C*, and the result of comparison is then reported to terminal *T*. The data transfer, in particular the transfer of *CODE*, the PIN and biometric data *BIO* to be described below, is preferably effected in encrypted form in order to protect said sensitive data from being spied out.

If the PIN comparison was positive ("*OK*"), terminal *T* continues the authentication process by now effecting the user-unique authentication by means of the user's biometric features. The user presents terminal *T* with a biometric feature, for example a fingerprint or the iris of an eye. The biometric feature is detected by terminal *T* and converted into biometric data *BIO* which are transmitted, preferably in encrypted form, to smart card *C*. There, the user's read biometric data are compared with biometric data stored on smart card *C*. In the case of a positive comparison ("*OK*"), terminal *T* is enabled for the entry of further user commands.

Claims

1. A method for authenticating a user (*U*) of a data carrier (*C*) for authorized use of the data carrier and for authenticating a data carrier terminal (*T*) for authorized accessing by the data carrier terminal of memory areas of the data carrier, comprising the following steps:
   - reading a secret code (*CODE*) from the data carrier (*C*) by the data carrier terminal (*T*), whereby the secret code (*CODE*) is stored on a memory location that can be accessed only by authorized data terminals (*T*) and/or can be decrypted correctly only by an authorized data terminal (*T*).
   - presenting the read secret code (*CODE*) to the user (*U*),
   - presenting a biometric feature (*BIO*) of a user (*U*),
   - comparing the presented biometric feature (*BIO*) with a biometric feature stored on the data carrier (*C*).
2. A method according to claim 1, characterized in that a PIN is in addition presented to the terminal (*T*), being compared with a PIN stored on the data carrier (*C*).
3. A method according to claim 1 or 2, characterized in that a fingerprint of a user (*U*) is used as the biometric feature (*BIO*).
4. A data carrier (*C*) for authenticating a terminal with respect to a user and the user with respect to the data carrier, comprising a first memory area in which a secret code (*CODE*) is stored such that the secret code can be read and/or decrypted and displayed by an authorized data carrier terminal (*T*), and a second memory area in which data are stored which serve to authenticate the user with respect to the terminal.
5. A data carrier according to claim 4, characterized in that a PIN is stored in a third memory area.
6. A data carrier according to either of claims 4 and 5, characterized in that the biometric data are generated by a fingerprint.

7. An authentication system comprising a data carrier (*C*) with memory areas and a data carrier terminal (*T*) for accessing the memory areas of the data carrier, characterized in that
   - the data carrier (*C*) has a first memory area for storing a secret code (*CODE*) and a second memory area for storing biometric data,
   - the data carrier terminal (*T*) has a first device which is authorized for reading the secret code (*CODE*) from the first memory area and/or for decrypting the read secret code (*CODE*) and for presenting the read secret code on a display, and a second device for reading biometric data (*BIO*), and
   - a device for comparing the read biometric data (*BIO*) with biometric data stored in the second memory area in the data carrier (*C*) and/or in the terminal (*T*).
8. An authentication system according to claim 7, characterized in that the data carrier (*C*) has a third memory area for storing a PIN.
9. An authentication system according to claim 7 or 8, characterized in that the stored biometric data are generated by a fingerprint.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
8. Februar 2001 (08.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/09849 A1

(51) Internationale Patentklassifikation[7]: G07F 7/10, G07C 9/00

(21) Internationales Aktenzeichen: PCT/EP00/07122

(22) Internationales Anmeldedatum:
25. Juli 2000 (25.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 35 945.8 30. Juli 1999 (30.07.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: MÖDL, Albert [DE/DE]; Walter-Kollo-Strasse 21, D-86368 Gersthofen (DE). STEPHAN, Elmar [DE/DE]; Danklstrasse 13, D-81371 München (DE). MÜLLER, Robert [DE/DE]; Hansjakobstrasse 80, D-81673 München (DE).

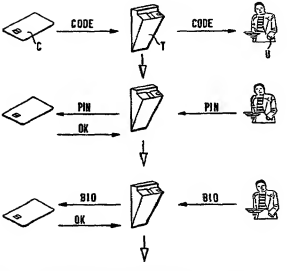
(74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzererstrasse 106, D-80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD, DATA CARRIER AND SYSTEM FOR AUTHENTICATION OF A USER AND A TERMINAL

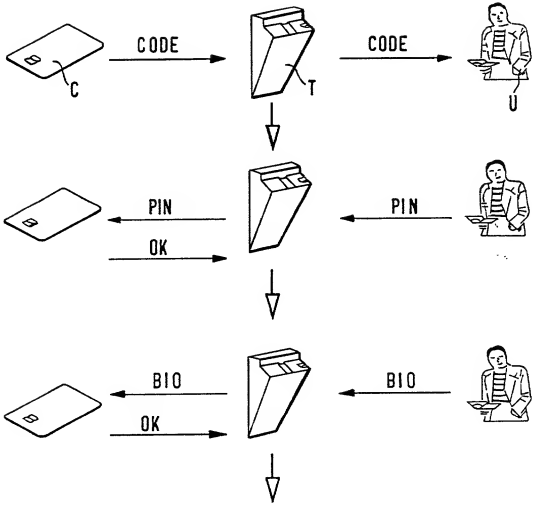
(54) Bezeichnung: VERFAHREN, DATENTRÄGER SOWIE SYSTEM ZUR AUTHENTISIERUNG EINES BENUTZERS UND EINES ENDGERÄTS



(57) Abstract: The invention relates to the use of data carriers such as chip cards C or similar. According to the invention, the terminal T which processes the chip card C first authenticates itself in relation to the user U and said user U subsequently authenticates him or herself in relation to the data carrier C or the terminal T. The authentication of the terminal in relation to the user U takes place by the readout of a CODE from the data carrier C and by the presentation of said readout CODE to the user U, who classifies this CODE as correct or incorrect. If the terminal T has presented a correct CODE, the user U authenticates himself in relation to the chip card C or the terminal T by presenting a biometric characteristic BIO, for example his or her fingerprint. This procedure ensures that the biometric characteristic BIO of the user U cannot be intercepted by a counterfeit terminal T.

[Fortsetzung auf der nächsten Seite]

WO 01/09849 A1


CODE
C
T
CODE
U
PIN
OK
PIN
BIO
OK
BIO

ATTORNEY/DOCKET NO: **MODL3003/JEK**

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:

METHOD, DATA CARRIER AND SYSTEM FOR AUTHENTICATING A USER AND A TERMINAL

the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **25 July 2000** ✓ as U.S. Application Number or PCT International Application Number: **(PCT/EP00/07122) 10/030,162** and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56*. I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No
199 35 945.8	Germany ✓	30 July 1999 ✓	X	

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	Day/Month/Year Filed

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker, Schmitt-Nilson, Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: Customer 23364

BACON & THOMAS, PLLC
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney**
(703) 683-0500

FULL NAME OF FIRST OR SOLE INVENTOR	CITIZENSHIP
Albert MÖDL	Germany ✓
RESIDENCE ADDRESS Walter-Kollo-Strasse 21, D-86368 Gersthofen, Germany DE	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW ☒
DATE X 22 March 2002	SIGNATURE X Albert Mödl

☒ *See following page(s) for additional joint inventors.*

ATTORNEY/DOCKET NO: **MODL3003/JEK**

CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

PRIOR FOREIGN APPLICATION(S) (35 USC §119)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E)	
Application Number	Day/Month/Year Filed

PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120)		
Application Number	Filing Date	Status - Patented, Pending or Abandoned

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
2- Elmar STEPHAN	Germany ✓
RESIDENCE ADDRESS Dankistrasse 13, D-81371 Munchen, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE → X 22 March 2002	SIGNATURE X E. Stph ←

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
3- Robert MÜLLER	Germany ✓
RESIDENCE ADDRESS Hansjakobstrasse 80, D-81673 Munchen, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE → X 22 March 2002	SIGNATURE X R. Müller ←

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

☐ *See following pages for additional joint inventors/priority applications.*